DOCUMENT RESUME

ED 345 710 IR 015 543

AUTHOR Okinaka, Russell T.
TITLE Virus Programs: A Clarification of Ideas and Strategies for Data Protection.
PUB DATE 13 Mar 92
NOTE 20p.; Paper presented at the Computer Technology Conference (San Bernardino, CA, March 13, 1992).
PUB TYPE Guides - General (050) -- Reports - Descriptive (141) -- Speeches/Conference Papers (150)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS Computer Networks; Computer Software; *Computer System Design; *Debugging (Computers); Disk Drives; Floppy Disks; Local Area Networks; *Microcomputers; Telecommunications
IDENTIFIERS *Computer Viruses

ABSTRACT

Virus programs have become a significant problem in the computer industry. The effects of these programs have been publicized widely. Anyone working with microcomputers cannot have escaped exposure to the term. Yet, there are a large number of people (teachers in particular) who have only vague notions of what viruses are. This paper provides a straightforward approach to the description of computer viruses, how they are transmitted and spread within computer systems, what viruses do once they are inside a computer system, and how computer systems can be debugged and protected against viruses. Computer systems are discussed at length, including hard disk drives, computer software, floppy disks, and computer networks such as local area networks. A glossary of important terms is included. (6 references) (DB)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it

☐ Minor changes have been made to improve reproduction quality

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy

Virus programs: A clarification of ideas and strategies for data protection

ED345710

Russell T. Okinaka, Ph.D.

California State University San Bernardino

5500 University Parkway

San Bernardino, CA 92407-2397

12015543

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
Russell T. Okinaka

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

BEST COPY AVAILABLE

Abstract

Virus programs have become a significant problem in the computer industry. The effects of these programs have been publicized widely. Anyone working with computers cannot have escaped exposure to the term. Yet, there are a large numbers of people (teachers in particular) who have only vague notions of what viruses truly are. It is clear that viruses pose a threat to legitimate computer users world wide. It would seem that a clear understanding of how viruses invade computer systems would help in limiting the scope of their effects.

With regard to computer viruses, the literature is filled with articles that are abstract and technical. Yet, if explained properly, it is possible to understand what viruses are, what they do, and how you can protect yourself against them. It is the purpose of this article to provide the reader with just this type of information. It is also intended that this information be presented in a fashion that is easily understandable and straight-forward. Technical terminology is to be kept to a minimum.

Introduction

If you are a person who does any kind of work with a personal computer or mainframe system, the term "computer virus" cannot have escaped your attention. The news media consistently talks about these programs which plague our society-- creating heart-ache and confusion among thousands of computer users. The number of viruses infecting systems has reached epidemic proportions throughout the world. Yet, there are a great many people who only have a vague notion of what a virus truly is. It is the purpose of this article to try and clarify the term, and provide understandable information on how to recognize and eliminate viruses from a computer system. Any myths surrounding these programs should also, hopefully, be eliminated.

Importance of this Paper

Although there are many articles and even books covering the subject of computer viruses, most, if not all of these references use intimidating technical jargon in their explanations. Often, one finds the need for a degree in computer science to understand many of the terms that are mentioned in such articles. This, unfortunately, results in little illumination for the average lay-person. One does not necessarily need to have an understanding of sectors, drums, tracks, and .com files to know what a virus is and the effects that it can have.

Teachers in particular, often have questions about the nature of virus programs. They usually understand that undesirable effects can result from having computer viruses on their systems. Many of these individuals, however, have misconceptions about how viruses work and how they are transferred from computer to computer.

If a person is knowledgeable about computer viruses, he can then take steps to reduce the chances that his computer system will become infected, rather than relying on misinformation, or simply ignoring the problem. Having a virus on your system does not have to be catastrophic. Ignoring the problem, however, can lead to serious problems. There are ways of minimizing the chances of being infected by a computer virus, removing

certain kinds of viruses that are already on systems, and protecting yourself in the event that you obtain a virus that cannot be removed for some reason. This can end up saving the computer user many from many hours of potential aggravation and frustration.

Definition of Terms

Certain terms should be familiar to the reader of this article before going into any great detail on the topic of virus programs. The following list should help you to better understand the material that is to follow.

RAM--An acronym for Random Access Memory. This is the main electronic memory of a computer system. This is often referred to as the computer's working memory. One of the characteristics of RAM is that it is volatile. This means that its contents are lost when the power is shut down.

Secondary Storage--This term refers to the magnetic storage that is used to keep permanent records of software and data files. The most common form of secondary storage is the *floppy disk*. Other forms include *hard disks*, which store information in ways that are similar to floppies, but have much larger data capacities. Hard disk drives are often *fixed and internal*. This means that they reside within the body of the computer, and cannot be removed without physically taking the computer apart.

Telecommunications--Communicating between two or more computer located a large distance apart over the phone lines. Communicating between computers requires a special device called a MODEM, which allows the computers to make use of the telephone lines as a communications medium.

Back up copy--This refers to a copy that is made of a piece of software or a data file. It is recommended that if you have a piece of software or a set of data files that you use frequently, that you copy the information to a "back up diskette." This is so that you have something to fall back on should something happen to your working copies.

Pirate Boards--This refers to electronic bulletin boards (telecommunications systems) which contain copyrighted software. Operators of these pirate boards disseminate the copyrighted material illegally to other users of the board.

Down-loading--This term refers to receiving information from another source via telecommunications. To "download" a file means that you are receiving the file from another computer.

Hacker--A person who uses the computer for illegal purposes. Hackers commonly attempt to gain unauthorized entry into external computer systems. Hackers are responsible for creating and disseminating many of the virus programs that are currently in existence.

Formatting--This refers to a procedure that is used to make capable of receiving information. Formatting essentially creates "addresses" which serve as storage areas for

data. The procedure is used for both hard disks and floppy disks. Occasionally, a disk will become damaged and will need to be re-formated. Re-formating a disk erases any information that was previously stored.

(Lockard and Abrams, 1987).

What is a Virus?

A virus is actually a computer program that is designed to "hide" on a disk. This means that a user will not know that a disk is infected when he uses it on a computer system. Viruses are also designed to *replicate* themselves. This means that they copy themselves from disk to disk as unsuspecting computer users work with infected computer systems. Viruses are usually designed not to manifest themselves immediately. The longer the programs can "hide," the more computer systems they can potentially infect.

Computer systems that are *most* susceptible to viruses are those which contain hard drives. If a person uses an infected floppy disk on a computer that is equipped with a hard drive, the virus will be transferred to the hard drive without the user's knowledge. Should another user place his floppy disk in the now infected computer system, his disk also become infected. If these users move on to use different computers, the virus can be spread over many machines in a short period of time.

This kind of problem can be especially severe in places of business, or in school settings, where there are computers that are used by many different individuals. For example, in a school setting, if a virus exists on a computer system, then all the users of that system during the day would end up having their floppy disks infected. The number of people using a particular computer in a school setting can be considerable. Therefore, it is easy to see how an "epidemic" could literally arise as the result of a virus existing on only one computer system. In this respect, computer viruses resemble their biological counterparts--that is in terms of their "contagiousness."

The reason why systems with "hard drives" are most susceptible is that these systems usually have all of their operating software pre-loaded. The hard disk provides a

place for the virus to hide. If there were no hard drive on the computer system, then there would be nothing to infect. On a system with NO hard drive, the system is essentially "purged" when the power is shut down. This is because the electronic memory of the computer is automatically erased when the power goes off (This is what is meant when it is stated that the computer's main memory--called RAM, which stands for Random Access Memory, is *volatile*). Since a virus is nothing more than a program, it is erased from memory when the power goes off (Some people believe that viruses can somehow linger in the computer's main memory even though the power has been shut down. This is a misconception.). When a hard drive is infected, on the other hand, the entire contents of the drive become threatened by the virus. Hard drives store information magnetically. Therefore, they will retain programs (including viruses) even *after* the power has been shut down (just as other software remains on the hard disk after you shut down the power). In a worst case scenario, this could mean that the disk needs to be reformatted, and its entire contents would have to be re-loaded. This commonly takes hours, and requires that all programs and files have been "backed up" on floppy disks. If no back-ups of the information have been made, the data might be lost forever.

What are the effects of Virus Programs?

The effects of a virus programs vary considerably. Some of these programs have catastrophic effects. Others are mere nuisances. Effects of virus programs include (but are not limited to) the following:

1) Causing your hard drive to be erased completely. This is the most undesirable of the effects because of the time involved in reformatting the disk and reloading software and data files. As mentioned before, some data may be irretrievable if back up copies have not been made (Simonson, Thompson, 1990).
2) Sending messages to the screen (this can be something unkind, or something

silly).

3) Causing your data files to be renamed or un-named. This can be a very irritating effect, resulting in the user having to determine the contents of each file, and to re-name them.

4) Causing your files to increase in size. This means that you start to suddenly run out of disk space, even if you haven't added any information to your files at all!

5) Causing your system to slow down. Some virus programs cause the system to behave very sluggishly. Some will slow down so much that very little productive work can be accomplished. The user also becomes quite irritable when such circumstances exist.

6) Changing icons such as mouse pointers into different pictures. Indeed, one AMIGA virus, known as *the Revenge* virus will wait one minute after each re-boot of the system, and then change the mouse pointer to resemble a certain part of the male anatomy (Roberts, 1988).

(See Appendix A for a list of some common computer viruses.)

As you can see, viruses can damage and destroy data. They can make working with a computer a very frustrating experience.

How do they work?

The ways in which viruses manifest themselves also vary depending on the type. Some show up when the computer has been booted up a certain number of times after infection. In such cases, counters are included within the virus programs so that the primary effect will be "triggered" after so many uses (For example, the primary effect might be noticed when the computer was used for the 50th time after infection). Such a virus could conceivably hide on a system for many months before it was detected. Other

viruses are triggered by the clock or the calendar that they read off the computer. Recently, the "Michelangelo" virus was set to go off on the birthdate of the famous artist (which was March 6th) (Elmer-Dewitt, 1992). Still others contain certain mathematical formulae which will modify themselves in a geometric fashion. Initially, the progression is slow. But as you proceed further into the sequence, the rate at which it amplifies increases at a greatly accelerated rate. An every-day example of a geometric progression is that of a person who starts with a penny on one day, and has his money doubled for every day subsequent to this for the period of a month. At the end of the month, this lucky person would be a millionaire many times over (See Fig. 1). Similarly, a virus which increases in size geometrically will ultimately take up all of the space on your disk, progressing slowly at first, and dramatically faster towards the end of its cycle.

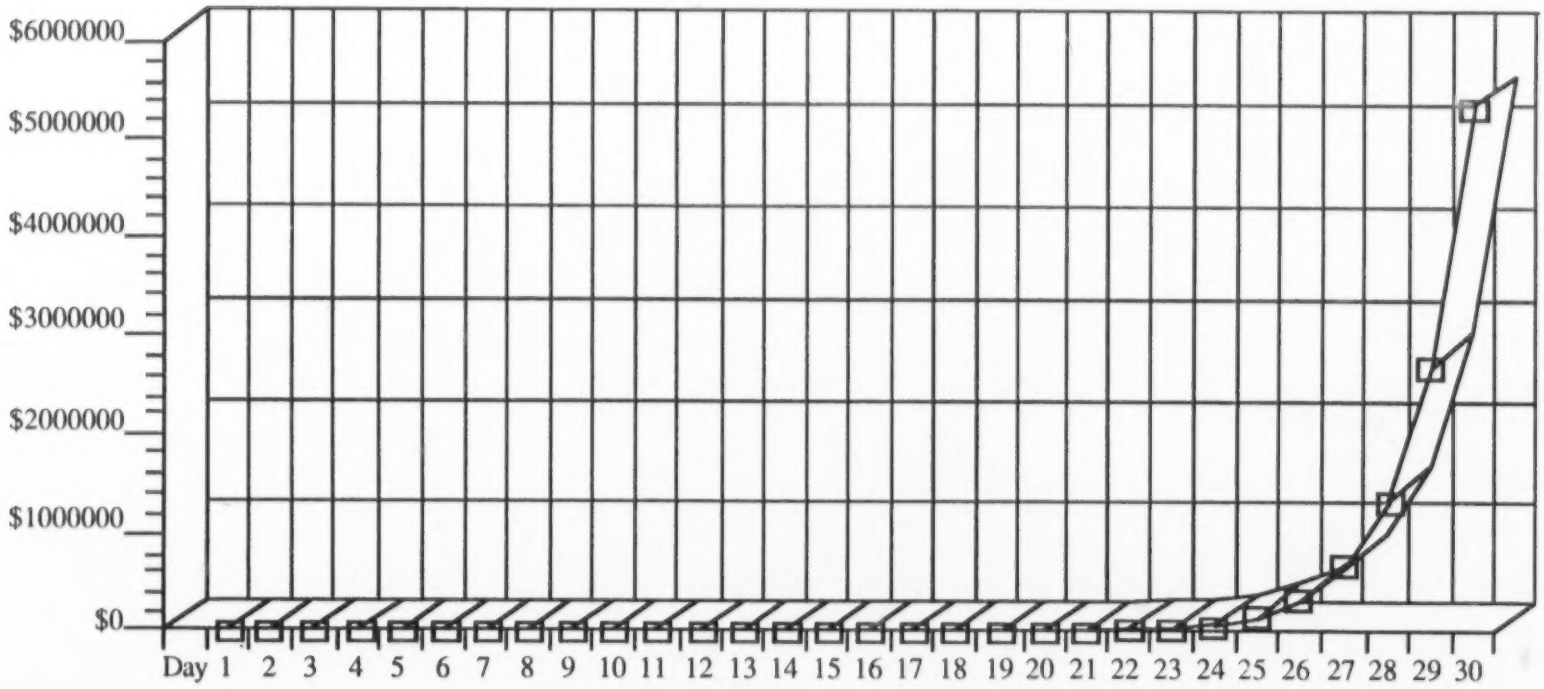
Some virus or virus-like programs are quite diabolical. In one instance, a disgruntled employee decided to leave a "bomb" on a mainframe computer system at the company where he worked. Upon terminating his employment with the company, he set the "bomb" to go off when his social security number was deleted from the payroll. This resulted in the program causing all of the company's hard disks to be erased (McKeown, 1987).

How do viruses get on to computer systems?

Viruses enter computer systems by several means. They can be loaded on to a system from an infected disk. They can also enter a computer system via a local area network. The third possibility is that they can infect a system that is actively engaged in telecommunications. Local area networks or LANs are systems that are set up where several computers are connected to a central "file-server." This is where software and/or data files may be obtained from a central PC which disseminates this information to the other computers that are physically cabled to the network. Telecommunications involves the communication between two or more computers located a large distance apart via the

Figure 1. Geometric Progression

- Progresses slowly at first.
- Rate of increase consistently accelerates.
- Rapid progression at the end.
- Graph below is the example of a person who has his money doubled every day for a month. Person starts with a penny and ends up a millionaire.



phone lines. Special devices known as a modems are necessary for computers to communicate with each other over the phone lines. In a network viruses may be transferred to other computers if one of the systems in the network is infected. With telecommunications, a person with the right kind of knowledge can infect *many* users very quickly . Indeed, there are "hackers," who deliberately attempt to load viruses to different computer systems via telecommunications. Some of these people have been successful in knocking out hundreds of computer systems in a single day. Information services such as Compuserve and Prodigy must continually be on the look out for people who try to infect their systems with virus programs. Clearly, there would be many disgruntled people if viruses were suddenly to infect the systems of subscribers.

Because telecommunications renders so many systems susceptible to infection, it is necessary for businesses, financial institutions, government agencies, colleges, and universities to monitor their systems to make sure that they do not become infected. This is a demanding, and highly responsible task, often requiring meticulous attention to detail.

Who creates virus programs?

People often wonder: "What kind of person creates virus programs and deliberately infects other systems?" The answer to this question is that there are certain elements in our culture which thrive on the darker side of the computer world. These people spend all of their time performing activities which are largely illegal. These activities include gaining unauthorized entry into external computer systems, performing computer crimes such as the manipulation of data and assets, and loading viruses on to computer systems for the purpose of attacking associated software and/or data.

Members of this culture consider the completion of these acts to be a sign of their prowess. The more systems they can invade, and the more insidious the means, the greater the achievement. It is similar to gaining rank within a warped or twisted organization.

Historically, the precursors to virus programs had their origins in the 1960s. During this period, there were no micro-computers in existence. People who were engaged in the use of computers worked exclusively on mainframes. Programming was the primary means by which most tasks were accomplished. These early programmers would sometimes play practical jokes on each other by writing small programs that would "sabotage" their colleagues. Programs that would cause another person's program to "crash" or "bomb" would be written with the intention of taunting fellow colleagues (Roberts, 1988). The more sophisticated the sabotage, the greater the respect the person would earn among his peers.

As microcomputers became widely available, the first virus programs also began to appear. At first, viruses were relatively rare, but as computers and computer software became more wide spread, so did the viruses.

Many software companies wished to keep viruses a secret, as knowledge of these programs had the effect of discouraging the use of microcomputers and software. Much was done to "hush up" the existence of virus programs.

There have been those who suggested that the original intent of some virus programs was to thwart software piracy. Causing the hard disks of pirate board systems to crash or to be reformatted would punish those who were actively engaged in infringing on program copyrights. The intent was to reduce the loss of income that software developers faced as a resulted of software piracy.

The reality of the situation, however, was that virus programs started to infect the systems of legitimate computer users. The costs that have resulted in terms of damaged software and lost time can be estimated in the millions of dollars (not to mention the anxiety and stress produced by the effects of these programs).

Is it illegal to deliberately load virus programs on to other computer systems?

The answer to this question is a definite YES! The penalties are especially severe for individuals who destroy government computer software and data, or information contained within federally insured financial institutions (McKeown, 1988). The *computer fraud and abuse act of 1986* makes it a crime to damage data in the institutions mentioned above. It also makes it a crime to view, copy, or damage computer data across state lines. Individuals convicted under this act can be fined up to $100,000.00 and serve a jail sentence of up to 20 years (McKeown, 1988).

The computer fraud and abuse act clearly covers the effects of many virus programs. The greatest difficulty in prosecuting, however, is isolating the creator of the program. If a virus can be traced to a specific source, then prosecution of the perpetrator can take place. This, unfortunately, can be a very difficult task. The truth is that the vast majority of individuals who are responsible for creating and disseminating computer virus programs go un-punished.

So how do I protect myself from virus programs?

You do not have to worry about viruses if all of the following conditions are satisfied: a) You are the only user of your computer; b) You never exchange disks with other people; c) You never buy new commercial software; and d) You do not use telecommunications. It is virtually impossible, however, to satisfy all of the conditions mentioned above--especially conditions a and c (Note: While it is possible to obtain a virus from a piece of commercial software, it is usually unlikely to come from this source. Viruses are far more likely to come from other sources like public domain software. There are examples, however, of computer systems that have been infected by commercially prepared disks. In some instances, the software companies have tried to cover up the fact that the viruses originated from their program disks.). It is possible, however, to limit your susceptibility to infection. This can be accomplished in the following ways.

First, you should never down load software from "pirate boards." Pirate boards are bulletin board services which disseminate commercially copyrighted software to anyone who wishes to have a copy of the software. Such boards are noted for transferring virus programs along with the pirated software.

Second, avoid swapping your disks with too many people. The more disks you exchange, the greater the chances are that you will obtain a virus from someone along the line.

Third, obtain some kind of virus protection software (See Appendix B). There are many commercially developed pieces of virus detection software. There are also several "public domain" virus detection programs. These programs can usually be set to scan disks as soon as they are placed into your disk drive. Attempts are made to locate any known versions of viruses that might be present on the disk. If a virus is detected, a warning will usually appear on your screen indicating that *a virus is present.* Some of these programs will allow you to "disinfect" your disk. This means that the virus detection software will remove the virus from the infected disk. It will do this by isolating and destroying the undesired code. Commercial virus detection programs are available for all major computer brands. These programs usually retail from $40.00 and up, and it should be emphasized that they are well worth this minimal investment. An important thing to note is that when you purchase a piece of virus detection software, you should *be sure to obtain the latest version.* Viruses constantly evolve, as hackers strive to develop strains that will penetrate the current versions of detection software. Therefore, the companies that market the detection software must constantly upgrade their software to detect the "latest viruses." Try to purchase the latest version only. You will generally be allowed to upgrade your software for a nominal fee as new versions are developed, provided that you keep your original proof of purchase.

Fourth, *and this is extremely important,* make sure you have back up copies of all of your software and data files. Even though this can be a tedious task, try to take the time

to back your data up on a regular basis. In the long run, you may find that this is the most valuable time you ever spent.

Conclusion

It is clear that virus programs are prevalent among many computer systems. The effects of these programs can be more than mere nuisance. Virus programs have the potential to completely disable your computer system and to destroy valuable data and software. They have the capacity to spread in ways that resemble their biological counterparts. Viruses can infect hundreds, or even thousands of machines in an extremely short time depending on how they are disseminated. The knowledge of how these programs are transmitted from one computer system to another, however, allows a person to take adequate precautions against their potentially catastrophic effects.

Computers with hard disk drives are the most susceptible to virus programs because they give the virus a place to reside once the computer's main memory is shut down. Because of the large data capacity of such drives, it can be extremely time consuming to re-initialize the disk and to re-load all of the software and data files that were damaged or destroyed.

The precautions which minimize the susceptibility of a computer system to virus programs include the following: *1) Never down-load programs from pirate boards; 2) Limit the frequency with which you exchange disks with other people; 3) Obtain a virus protection program, or disinfectant; and 4) Make sure your software and data are backed up*.

Because virus programs are unlikely to disappear in the near future, it behooves an individual to follow these relatively simple recommendations. While this does not guarantee that your life will be unaffected by virus programs, it does greatly reduce the chances that you will suffer the results that might be inflicted under a worst case scenario.

Thus, the chances that you will continue to work productively with your computer, which is a wonderful and extremely powerful tool , are enhanced considerably.

Appendix A--Virus Protection Programs*

MacIntosh	*Sugg. Retail*
SAM Intercept	$59.95
Virex	$59.95
AntiToxin	$99.95

IBM & Compatibles

Bomsqad	Freeware
C-4 Antiviral Shield	$40.00
Caware	Shareware
Checkup	Shareware
Condom	Public Domain
Cop	Shareware
Data Physician	$199.00
Disk Defender	$240.00
Disk Watcher	$99.95
Dr. Panda	Shareware
Flu_Shot	Shareware
Ice	Public Domain
IFCRC	Public Domain
Mace Vaccine	$20.00
NoVirus	Shareware
SYSCHK	Shareware
Softsafe	$99.00
Tracer	$49.95
Trojan Stop	Public Domain
Vaccine	N/A
Tracer	$49.95
Vaccine from World Wide	$79.95

AMIGA

VirusX
Clockdoctor
Killvirus
Sentry.zoo
The_Virus
TCELL
Viewboot
Warp
Protection

Note: The list of AMIGA anti-virus programs shown here were listed in the directory of the professional information service known as GEnie, which is run by General Electric. By becoming a member of this service, it would be possible to download these programs to your computer.

*Virus programs may be obtained from software stores, or through mail order in computer magazines. Each of the major PC types have magazines or journals devoted to that specific platform.

Appendix B--Viruses Commonly Found on Different Computer Systems

MacIntosh

nVIR	Hpat	INIT29	PEACE
ANTI	MEV#	AIDS	Scores
nFLU	J-NVIR	Trojan Horse	CDEF
WDEF B	ZUC	ZUC B	ZUC C
MDEF	MDEF C	MDEF D	ANTI
Hpat			

IBM & PC Clones

Brain	Lehigh	Friday the 13th	Sunnyvale Slug
Retrovirus	Michelangelo	Trojan Horse	Bombs

AMIGA

SCA	Obelisk Softworks Crew	Byte Bandit	Revenge
Byte Warrior	Clock Virus		

Note: This lists above are by no means comprehensive. Estimates of the total number of virus programs in existence extend into the *thousands*. The lists above merely mention some of the more common or notorious virus programs that have infected computers.

References

Elmer-DeWitt, P. (1992). Ding! Whrrrrrrrrrrr. Crash! *Time*, 139 (4).

Lockard, J., & Abrams, P., (1987). *Microcomputers for educators*. Boston, Massachusetts: Little, Brown & Compsny.

McKeown, P. (1987). *Living with computers*. New York, Harcourt, Brace, Jovanovich.

Moursund, D. (1989). A computer virus. *The computing teacher*, 16(6). 4.

Roberts, R. (1988). *Computer viruses*. Greensboro, COMPUTE Publications Inc.

Simonson, M and Thompson, A. (1990). *Educational computing foundations*. Columbus, Merrill Publishing Co.